情報セキュリティ自己診断チェックリスト
～情報セキュリティ対策　12カ条～

このチェックリストでは、パソコンやスマートフォンなどの機器を利用する場面ごとに、情報セキュリティに関して知るべきこと、やるべきことをまとめました。本チェックリストを用いて、みなさんの情報セキュリティ対策を確認してみましょう。

内閣官房情報セキュリティセンター

1. 利用環境の設定
パソコンやスマートフォンには、コンピュータウイルスの感染防止のためのウイルス対策ソフトを導入していますか？

2. パスワードの設定
自分のパソコンやスマートフォンには、他人が容易に推測できないパスワードを起動画面に設定することにより、他人が利用できないようにしていますか？

3. セキュリティの更新
パソコンやスマートフォンのOS(オーエス)※やソフトウェアを更新して常に最新の状態を保っていますか？（※用語解説参照）

4. 紛失したら困る重要情報の取り扱い
紛失したら困る重要情報（電話番号や電子メールアドレス、思い出の旅行写真などの画像データなど）には、パスワードをかけたり、複製（バックアップ）をしていますか？

5. 個人情報の公開範囲の設定
自分や家族、友人の個人情報をSNS(エスエヌエス)※やブログに掲載するときは、情報を伝えたい人にだけ公開するよう、適切に公開範囲を設定していますか？

6. 家族や友人の個人情報の取り扱い
家族や友人の名前やメールアドレス、一緒に撮った写真などをインターネット上に公開するときは、事前に本人の許可を得ていますか？

7. 金融財産情報の取り扱い
金融機関を名乗り、口座番号や暗証番号、クレジットカード情報の入力を促すようなメールがきた場合、安易にそれらの情報を入力しないよう注意していますか？

8. デジタルコンテンツの入手・視聴
スマートフォンのアプリケーション※は、OSを提供している事業者や携帯電話会社などが、安全性の審査を行っている信頼のおける場所から入手していますか？

9. 電子メール利用時
身に覚えのない電子メールには、コンピュータウイルスが潜んでいる可能性があることを認識したうえで、添付ファイルを開かないなどの対応をしていますか？

10. 自宅外利用時
パソコンやスマートフォン、USBメモリなどを持って外出するときは、機器やファイルにパスワードを設定し、なくしたり盗まれたりしないよう気を付けて持ち歩いていますか？

11. トラブル発生時
架空請求の電子メールが大量に届いたり、開いているウェブページをどうしても閉じることができない場合、1人で悩まず誰かに相談していますか？

12. インターネット接続機器利用時
インターネットに接続したテレビやゲーム機器でネットショッピングなどのサービスを利用するときは、ウイルス感染などの脅威に遭う可能性があることを想定して、セキュリティに配慮していますか？

◆用語解説

OS(オーエス)	オペレーティングシステムの略称で、パソコン全体を管理するためのソフトウェアです。具体的には、キーボードの入力やディスプレイ、プリンタへの出力といった入出力機能などの管理を行っています
SNS(エスネヌエス)	SNSとはソーシャルネットワーキングサービスのアルファベットの頭文字をとったもので、個人の日記やフォトアルバムを特定の人に公開できたり、利用者同士が気軽に意見交換できるコミュニティを開設できたりなど、様々な機能を持ったウェブサイトを提供するサービスです
アプリケーション	文書の作成や数値計算など、ある特定の目的のために設計されたソフトウェアです。どのソフトウェアにも共通する基本的な機能をまとめたOSに、ユーザが必要とするものを組みこんで利用します
ワンクリック詐欺	不当な料金請求の手法の1つで、アダルトサイトや出会い系サイトなどにアクセスしたときに、いきなり料金請求の画面が表示されるという手口の詐欺です

◆各種相談窓口

● 購入した製品の具体的な使い方については取扱説明書などに記載されている連絡先へご連絡ください
　✓各製品の開発元/販売元
　✓電話番号　各製品の取扱説明書などに記載されています

●コンピュータウイルスに感染してしまったと思ったらこちらにご相談ください
　✓IPA(アイピーエー)(情報処理推進機構)セキュリティセンター　安心相談窓口
　✓電話番号　03-5978-7509　(平日10:00～12:00 および 13:30～17:00)

●広告や宣伝目的の迷惑メールに困っている時はこちらへご連絡ください
　✓財団法人日本データ通信協会　迷惑メール相談センター
　✓電話番号　03-5974-0068　(平日10：00～17：00)(祝祭日は除く)

●犯罪に係る相談や情報提供を電話で受け付けています
　✓各都道府県警察のサイバー犯罪窓口
　✓電話番号　各都道府県警察にお問い合わせください

◆さいごに
みなさんはいくつチェックできましたか？　全てにチェックできるまで繰り返し確認し、安全・安心なデジタルライフを送りましょう。

～解説～

1. 利用環境の設定

パソコンがコンピュータウイルスに感染すると、悪意のある人にパソコンを操られて他のサイトへの攻撃に悪用されたり、プライバシーに係わる大切な情報やクレジットカード番号などの金融情報が漏えいするなどの被害を受ける危険が発生します。

コンピュータウイルスの感染を防ぐために、ウイルス対策ソフトを導入しましょう。（ウイルス対策ソフトは家電量販店などで入手することができます。）

2. パスワードの設定

パソコンやスマートフォンの起動時のパスワードを設定していないと、自分以外の人に機器を利用される危険があります。

自宅に鍵をかけるように、自分だけが利用できるように起動時のパスワードを設定しましょう。パスワードには、住所や電話番号、誕生日のような他人から推測されやすい情報は使用しないようにし、もし、忘れないようにメモに残さざるをえない場合は、人の目に触れない場所にメモを保管するようにしましょう。

3. セキュリティの更新

パソコンやスマートフォンのOSやソフトウェアに存在する情報セキュリティ上の欠陥を“セキュリティホール”と言います。これらにセキュリティホールがあると、たとえウイルス対策ソフトを導入していても、インターネットに接続しただけでコンピュータウイルスに感染してしまうことがあります。

このような被害を防ぐためには、OSやソフトウェアは常に更新し、最新の状態にしておくことが重要です。OSやソフトウェアの更新は自動更新に設定しておくと便利です。

4. 紛失したら困る重要情報の取り扱い

次の情報は、インターネット上にひとたび公開されると、プライバシーを侵害されるなどの精神的な苦痛を受けるかもしれません。

【個人情報】氏名、誕生日、住所、性別、体重、メールアドレス、電話番号、学歴、病歴など
【思い出情報】家族や友人と写った旅行写真や動画、想い出に残る物や景色の写真など

漏えいすると困るファイルなどにはパスワードをかけておくとよいでしょう。

また、消えてしまうと取り返しのつかない思い出情報を含むファイルなどは復元できるようにUSBメモリなどにバックアップを取っておくなどの対策が有効です。

5. 個人情報の公開範囲の設定

SNSやブログでは、個人情報を公開するときに公開する範囲を制限することができますが、それを知らずに利用している人も中にはいます。自分自身のスケジュールや家族や友人と撮った思い出の写真を公開範囲を制限せずに一般公開してしまうと、自分をはじめ、家族や友人も、不特定多数の人からプライバシーを侵害されるかもしれません。

SNSやブログで自分や家族、友人の個人情報を公開するときには、自分が情報を伝えたい人にだけ公開範囲を制限しましょう。

6. 家族や友人の個人情報の取り扱い

自分の個人情報を漏えいしないように取り扱うことは大切ですが、家族や友人の個人情報を知らぬうちに勝手に公開しないなどの配慮も大切です。例えば、家族や友人と一緒に写った写真や動画は、あなたの情報でもあり家族や友人の情報でもあります。あなたの判断で良いと思って公開した情報であっても、家族や友人からしたら公開して欲しくない情報かもしれません。

家族や友人の個人情報をインターネット上に公開するときは、情報を公開しても良いか、本人から事前に許可をもらうようにしましょう。

7. 金融財産情報の取り扱い

金融機関などになりすまして、口座番号や暗証番号、クレジットカード情報などの入力を促すようなメールを送り、財産をだまし取ることを“フィッシング詐欺”と言います。

フィッシング詐欺の被害に遭わないためには、口座の暗証番号などの入力を催促するメールが届いても、覚えのないメールは返信せず、通帳やカードに記載されている金融機関の連絡先に事実確認を行うなど、安易に口座番号や暗証番号などの金融財産情報を伝えないことが大切です。

8. デジタルコンテンツの入手・視聴

インターネット上には映像や動画を入手したり視聴する環境が充実しています。
一方で、悪意ある人がコンピュータウイルスを忍ばせたアプリケーションを提供し、利用者がダウンロードし実行してしまったことで、ウイルスに感染してしまうことがあります。ウイルスによって、パソコンの中にあるファイルやソフトウェアが壊されたり、情報が盗まれたりする被害も発生しています。

上記のような悪意のあるアプリケーションによる被害を回避するために、安全性の審査が行われているサイトからデジタルコンテンツをダウンロードしましょう。

9. 電子メール利用時

知らないアドレスから届く電子メールには、家族や友人からのアドレス変更通知やショッピングサイトからのダイレクトメールだけでなく、架空請求などの悪意のあるメールもあります。

このような電子メールにはウイルスが潜んでいる可能性もあります。ウイルス感染を防ぐためには、身に覚えの無い電子メールの添付ファイルは開かないなど、慎重な行動が大切です。

10. 自宅外利用時

外出先でパソコンやスマートフォンをうっかり紛失したり盗まれたりすると、機器の履歴からネットバンキングやネットショッピングへのアクセスを試みられたり、電話帳に登録している友達に迷惑をかけてしまうかもしれません。

例えば、外出先のお店でパソコンやスマートフォンを利用しているときは、少し席を外すのであれば、盗難を防ぐために機器を持って移動しましょう。また機器が盗難されても中の情報が悪用されないように、起動時のパスワードは設定するようにしましょう。

11. トラブル発生時

インターネット利用に関する被害相談として、ワンクリック詐欺※に遭ったり、架空請求の電子メールが大量に届いたり、開いているウェブページをどうしても閉じることができないというような事例が増えているようです。

このような症状が見られたら、１人で悩まず、誰かに相談しましょう。近所に住むセキュリティに詳しい人に相談したり、症状に応じて各種相談窓口に相談すると、よりスムーズにトラブルに対処できるでしょう。

12. インターネット接続機器利用時

インターネットに接続したテレビやゲーム機（以下、情報家電）には、情報検索やネットショッピングなど、パソコンやスマートフォンと同様のインターネットサービスを利用することができるものもあります。このことは、同時にウイルス感染などの情報セキュリティに関する被害に遭う可能性があることを意味します。

このため、まずは情報家電の取扱説明書に書かれているセキュリティ設定を適切に実施することが大切です。